Critical Infrastructure Protection in the Netherlands

The Dutch approach on CIP

Ministry of the Interior and Kingdom relations

Contents

1 The Dutch approach on CIP

Summary

This second report on Critical Infrastructure Protection (CIP) in the Netherlands gives an overview of the Dutch approach on CIP. In the report the backgrounds of the project are explained, the distinguished starting points are highlighted and a description of how the Netherlands have organised CIP is included.

During the first phase of the project a Quick Scan was performed to map out the critical sectors, products and services in the Netherlands. The outcomes of the Quick Scan served as the basis for the next phase of the project. This next phase is elaborated into three sub projects:

1 Identifying critical junctions (also in terms of geographic location) between critical sectors and services.
2 Mapping out the vulnerability of sectors and junctions. Obtaining insight into protective measures already implemented.
3 Developing a cohesive set of protective measures, including any additional protective measures and embedding the measures to protect critical infrastructures within the standard business operations of the government and business community.

These sub projects are further explained in the report as well.

Finally, this document discusses the state of affairs of the project. The first sub project is already underway. In March 2004 a list announcing the junctions between critical sectors and services (also in terms of geography) has been presented to the Parliament. The Parliament is informed that this list of junctions is neither exhaustive nor definitive. Refining the list will stay possible during the implementation of the vulnerability analysis.

The Parliament is notified as well that involved parties gained a clear understanding of the complexity of the subject. Accordingly, there is a broad consensus about the fact that the protection of critical infrastructure isn't a once-only activity. CIP needs continuous attention, for it must be seen as a cyclical policy-process. This means that, although the project will end in June 2004, the ministries involved will continue to work on finalising and maintaining the set of measures.

2 Introduction

Started in April 2002, the Dutch project on CIP aims to map out and reduce the vulnerabilities of critical infrastructures in the Netherlands. As such, this project helps to enhance the protection of critical infrastructures against failure and disruption. Extensive in scope, the Dutch CIP project – under the management and co-ordination of the Ministry of the Interior and Kingdom Relations – involves the close co-operation of all of the ministries, the business community and lower tiers of government. According to the timeline, the project will be completed in June 2004. The project is not limited to generating an outline of and implementing a set of ad hoc measures. Perfecting, updating and monitoring the measures will also be essential, especially after project completion. The protection of critical infrastructure is an ongoing developmental process.

During the first phase of the project, a Quick Scan was performed to map out the critical sectors, products and services in the Netherlands and to give insight in their interdependencies. The findings of the Quick Scan, which was performed in close collaboration with the Netherlands Organisation for Applied Scientific Research TNO, are presented in '**Critical Infrastructure Protection in the Netherlands,** Quick Scan on Critical Products and Services.' The outline of the Quick Scan was approved by the Parliament. After this, the findings of the Quick Scan were used in elaborating the next phase of the Dutch CIP project.

This report is meant to provide more detailed information regarding the Dutch CIP project and the specified sub projects.

3 The Dutch CIP project

3.1 Background

For quite some time, the government and business community have been aware of the fact that certain critical public services are growing more and more dependent on the availability and reliability of other critical public services (including ICT). The Y2K problem in particular underscored this trend. In the spring of 2001, this awareness led the government to request the establishment of a cross-sector approach to protect critical infrastructures.

The horrific events that took place in the United States on 11 September 2001 highlighted the interdependence and vulnerability of critical infrastructures. The attacks on the World Trade Center and the Pentagon led to the establishment of the Action Plan on Security and Combating Terrorism, which incorporated the above request as Action Point 10.

Although its incorporation into the Action Plan may lead one to think otherwise, the Dutch CIP project does not focus exclusively on mitigating and preventing the consequences of terrorist attacks. The project also assesses situations that result from natural disasters, organisational or technical failures and human acts (both deliberate and accidental), against which the critical infrastructures of the Netherlands must be protected.

Action Point 10 states that the Dutch CIP project must result in the following:
(1) a cohesive set of measures, developed under the leadership of the Minister of the Interior, to protect the infrastructure of government and business and industry (including ICT)
(2) incorporation of the measures to protect critical infrastructures within the regular business operations of the government and business community.

3.2 The CIP project

The Minister of the Interior and Kingdom Relations was appointed as the co-ordinating project owner. Accordingly, the ministry also bears responsibility for achieving the objective and ensuring cohesion of the project results. The ministries involved bear responsibility for the activities they carry out. A project organisation within the ministry of the Interior has been established to manage and co-ordinate the various activities.

The protection of critical infrastructures affects of every ministry. Accordingly, each ministry is involved in the project. As described in TNO's Quick Scan report, the following sectors are deemed 'critical': energy, telecommunications, drinking water, food, health, financial, retaining and managing surface water, public order and safety, legal order, public administration and transport. These sectors are closely intertwined. Failure or disruption of one sector endangers the continuity of the sector in which the failure or disruption occurs. Moreover, it can also have major consequences for the continuity of the production processes of other sectors.

Most of the infrastructures listed above are partly, and in some cases entirely, managed by the business community and lower tiers of government. As a result, the project activities require not only consensus within the national government, but also with the business community and lower tiers of government. In this project, the business community is represented by the

Critical Infrastructures Co-ordination Committee, comprising representatives of the Confederation of Netherlands Industry and Employers (VNO-NCW). The lower tiers of government are represented by the Association of Netherlands Municipalities (VNG), the Association of Provincial Authorities (IPO) and the Association of Water Boards (UvW). These organisations play a key role in the critical sectors 'public order and safety' and 'public administration'. In addition, the ministerial bodies that perform the activities related to the CIP project maintain direct contact with the trade organisations and sectors involved.

3.3 Elaboration of the next phase of the CIP project

3.3.1 Starting points

The project's next phase has two aims: (1) clearly outlining the vulnerabilities that endanger the availability and continuity of the supply of critical products and services and (2) mapping out the protective measures already taken. Based on this insight gained in this phase the Dutch government can determine whether additional measures need to be taken. A number of starting points play a key role in the implementation of the next phase of the project.

Scale

The project addresses macro-level disruptions – the disruption or failure of a critical sector's service or product creates economic or social disturbances at the national or international level and can directly or indirectly impact the lives of many individuals. The disturbance is long-term, recovery requires a great deal of time and, during the recovery, there are few effective alternatives available. As a result, the CIP project addresses the top end of the disaster spectrum.

Scope

Regarding the list of critical products and services, a broad approach was used during the first phase of the project. Thanks to this broad approach in-depth insight into the interdependencies of critical products and services was yielded. To emphasize these interdependencies, the CIP project decided to maintain this broad approach in the next phase as well. Instead of making a priority, the vulnerabilities and protective measures for all critical products and services are mapped out. Nevertheless, certain decisions were taken to increase the manageability of this approach. The descriptions of the sub projects presented below reveal that the next phase involves an approach that was just as broad, but not as exhaustive.

Regular supervisory bodies ensure continuity within the government and business community as well. For this reason the project does not specifically focus on the areas of continuity under normal conditions, which are addressed by these supervisory bodies. Small-scale failures or disruptions are likewise not considered. Although the tasks and authorities of the normal sector supervisors – in so far as these are related to the protection of critical infrastructures – will be mapped out, no substantive assessments will be performed as part of the project.

It must be made clear that the government cannot guarantee that critical infrastructures will never fail or be disrupted. After all, modern-day life involves risks. However, the consequences of failures or disruptions will be reduced using the knowledge gained from and practical measures implemented as a result of the CIP project.

Ambition level

With regard to the protection of critical infrastructures in the Netherlands, the professional and political ambition level aims to ensure that the government and business sector take responsibility and work together to:
(1) do everything possible to prevent the large-scale failure or disruption of critical infrastructures (prevention)
(2) ensure that the Netherlands is properly prepared for the consequences should such a failure or disruption occur (preparation)
(3) take effective measures to minimize the loss that occurs as a result of failure or disruption (repression)

Responsibility

The ministries and business sectors bear responsibility for implementing the sub projects in the next phase and achieving the results envisioned in a timely manner. The ministry of the Interior continues to bear responsibility for overall co-ordination, ensuring project progress and consistency.

3.3.2 Division into sub projects

The third progress report of the Action Plan on Security and Combating Terrorism announced that the project objectives would be achieved with the performance of a number of follow-up steps. These steps are presented in the last English report as well **('Critical Infrastructure Protection in the Netherlands, Quick Scan on Critical Products and Services'**, page 10). After completion of the Quick Scan, this approach was further elaborated and simplified on a number of points, enabling to achieve the final results in a more effective manner. Thanks to the selected approach for the next phase the work is divided into a number of sub projects, which are described below:

1 Identifying critical junctions (also in terms of geographic location) between critical sectors and services. Part of the network of industrial and policy processes, junctions occur at the crossroads of critical products or services, which are either completely or largely interdependent. This level of dependence is described in the Quick Scan report. Geographic junctions involve spatial groupings of critical products and services.

Identification is necessary as a starting point for the determination of junctions between critical sectors and services. This list of junctions must offer a clear view of the critical sectors and services involved, the vulnerability of which at the very least must be investigated.

2 Mapping out the vulnerability of sectors and junctions. Obtaining insight into protective measures already implemented.
Scenarios are used to identify and map out vulnerabilities. In this process, the critical sectors and junctions will at least be assessed in terms of vulnerabilities that are the result of:

- technical or organisational problems (i.e. a wide range of human and material factors that play an essential role in the continuity of critical products and services);
- deliberate or accidental human action;
- natural disasters.

The ministries perform the vulnerability analysis as an extension of sub project 1. Because the circumstances in each sector differ a lot, it is difficult to develop a uniform, project-wide approach. Therefore, the manner in which the vulnerability analysis will be implemented is determined on a sector-by-sector basis. It is essential that the scenarios will be applicable in as

broad a manner as possible. They must be tailored in order to reveal as many of the sectors' vulnerabilities as possible. In addition, the scenarios must reflect the nature of the sector itself as much as possible in order to generate a good impression of the sector's possible vulnerabilities.

Depending on available capacity, security consultants from the General Intelligence and Security Service can be called upon to support the implementation of the vulnerability analysis.

As part of the vulnerability analysis, the ministries and business sectors will review which protective measures have already been taken. Accordingly, this phase will yield a representative view of the degree to which the critical sectors and identified junctions are vulnerable, which protective measures have already been taken and where shortfalls are apparent. In consultation with the other tiers of government, social partners and business community, the ministries will consider the effect of protective measures on the vulnerabilities and shortfalls identified. Rounding of sub project 2, these considerations will be assessed by the Dutch Cabinet. Eventually they will serve as the foundation for proposals for any additional measures, formulated by the Cabinet.

3 Developing a cohesive set of protective measures, including any additional protective measures and embedding the measures to protect critical infrastructures within the standard business operations of the government and business community.
To facilitate the decision-making process for the Dutch Cabinet the ministries will elaborate solutions for any shortfalls in consultation with the other tiers of government involved, social partners and the business community. These solutions will be based on the Dutch Cabinet's assessment and with due consideration of the vision of the Parliament regarding the findings of the CIP project. An integral component of the ministerial proposal is the division of responsibilities and authority regarding the protection of critical infrastructures and financing the measures (including additional measures) to be taken.

The policy surrounding the protection of critical infrastructures is comprehensive and complex. It involves a developmental process that will be further elaborated and perfected in the years to come. It is not realistic to expect the development of a comprehensive package of protective measures to be completed by June 2004 due in large part to the interdependencies of nearly every critical infrastructure, both in a national and international context.

3.3.3 Supporting sub projects

Using examples of good practice

In addition to the three subprojects listed above, examples of good practice from home and abroad are inventoried and exchanged throughout the project. These examples of good practice are not only applicable to different areas within the sector, but can also be exchanged between sectors.

Several meetings have already been held to explore the possibility of exchanging knowledge and experience with regard to examples of good practice. The aim is to increase the level of knowledge exchange between critical sectors. This type of exchange is already taking place at the international level, not only among participating consultation channels within the ministry of the Interior and other ministries, but also those of the EU and NATO. Bilateral

discussions, held in the past period, brought to the fore such issues as the many similarities in approach. Knowledge exchange on international level will be intensified in the near future.

Managing public confidence

During the next phase, the CIP project focuses heavily on increasing public confidence and increasing citizens' ability to deal with the failure or disruption of critical infrastructures. The manner in which the public is informed about the project will contribute to this.

Nowadays, the public has access to a great deal of information via various media channels (i.e. television, radio and the Internet). A government that is reluctant to provide information is no longer possible in today's world. In the current risk society, it is essential to be open and honest with the public. A pro-active approach in informing the public, companies and organisations about legislation and policy enhances the faith and trust of the public and companies in government. Clearly formulated information better educates the public about what they can expect from the government and where its responsibilities end. In addition to the pro-active provision of information, reliable follow-up information is also essential. When disaster strikes, the public has a right to receive clear and unequivocal information. This can reduce administrative risks.

Open and honest provision of information to the public is a general starting point. However, sensitive government and industrial information will be treated confidentially. Within the CIP project, information must be treated with care. Data regarding vulnerable aspects of critical infrastructures collected as part of the project are, after all, confidential.

Accordingly, it is clear that well-substantiated decisions must be taken with regard to what information should be made public and how this should occur. In addition, the desirability and necessity of making information public will be considered. With due regard for confidentiality, specific information regarding the outcomes of the three part projects will be made public only on an aggregate level.

The 'public's awareness of risk' is another theme that is inextricably linked to the CIP project. The public can expect the government and business community to map out and continually analyse the risks and to maintain, implement and update the protective measures agreed upon across the entire system. Besides, it must learn to deal with imperfect systems, unexpected events and the uncertainties of life.

4 Legal task force

In June a legal task force – chaired by the ministry of the Interior – began work. The taskforce will make recommendations about initial and additional measures to be taken to protect vital infrastructures, as seen from a legal perspective. These recommendations will be based on insight into the vulnerabilities and associated measures.

To assess the legal vulnerability, the broad outlines of relevant laws and regulations, including emergency legislation, will first be inventoried. Based on that inventory, the legal task force will make recommendations for possible amendments. At the same time, the task force will put forward its vision for the division of responsibilities among the public and private sectors.

5 Public-private division of responsibilities

In nearly every infrastructure deemed 'critical', products and services are provided by both public and private organisations. Accordingly, a key issue in protecting critical infrastructures involves how to best divide responsibilities and authority between the public and private sector. If responsibilities are not clearly delegated, it may involve major risks in crisis management. This key issue is decisive for the success or failure of the CIP project. After all, the question of how to divide responsibility is quickly followed by the question of who will finance any additional measures. At the moment, the division of responsibility is being worked out. A commission comprising representatives from the business community – the Critical Infrastructure Co-ordination Committee-is established specifically for this purpose.

The existing consultation structure with the VNO-NCW is continued during the next project phase. The business community does not only remain involved in the general co-ordination of the policy areas, but also at the sectoral level. Accordingly, the government must clearly outline the benefits to be gained by the private sector. To begin with, the government should stress the importance of continuity, which will attract new business. In addition, the establishment of an information exchange network for the drinking water sector, for instance, should be promoted.

As already indicated, in June 2004, a legal task force began working to assess the vulnerability of critical infrastructures from a legal standpoint. The division of responsibilities between the public and private sector is one of the specific issues addressed by this task force. Before making any findings public, an inventory of laws and regulations governing crisis management must be performed. The topic of confidentiality will also be addressed by the legal task force.

5.1 Confidentiality

With regard to the levels of confidentiality envisioned, the outcomes of the subsequent project phases will only be made available to the government bodies and companies that have a direct interest in it. This should guarantee the security of confidential company information as well.

6 State of affairs

6.1 Project progress

The sub projects have been further elaborated by the ministries involved. Initial steps for implementation of the sub projects have been made by the sectors. Sub project 1, addressing the junctions within and between critical sectors, is already underway. To maintain the possibility to compare the outcomes as much as possible, the analyses are implemented according a uniform framework. In March 2004 a list announcing the junctions between critical sectors and services (also in terms of geography) has been presented to the Parliament. The Parliament is informed that this list of junctions is neither exhaustive nor definitive. Refining the list will stay possible during the implementation of the vulnerability analysis. The outcomes so far can be seen as a deepening of the insight into the critical infrastructure. Moreover, they serve as a valid foundation to start the vulnerability analysis.

The outlines of the approach of the vulnerability analysis are recently approved by the ministries. These analyses will soon be started, some ministries have already begun. It heavily depends on the complexity of the sector what the duration of the analysis will be.

It appears that the extensive nature and complexity of the issues necessitate a slight adjustment of the timeline. For the parties involved, the top priority is not the speed with which the project is completed, but the optimal protection of critical infrastructures in the Netherlands. For this reason, the Dutch government has taken the decisions that in June a cohesive, but not exhaustive, package of protective measures will be presented to the Parliament. At all levels, the ministries involved will continue to work on finalising and maintaining the set of measures after the project has ended in June.

The Dutch CIP project is a continuous policy process that will never be perfected, but the government, business community and larger public will have to learn to accept these imperfections, as well as the risks and uncertainties these entail. In June 2004 more detailed information regarding the outcomes (available at the time) of the sector-specific vulnerability analyses will be presented. This information should offer the first insight into the vulnerability of critical infrastructures in the Netherlands.

6.2 Policy regarding the long-term protection of critical infrastructures

In view of the information presented above, the second project objective and in co-operation with all the parties involved, we are currently working to determine the most effective way to achieve and maintain the protection of critical infrastructures after the project has ended. Taking into account the efforts of other countries in the field of protecting critical infrastructures (also in the context of EU and NATO efforts), it is essential that this policy field become a standard part of policy after June 2004. At the same time, losing the knowledge generated must be avoided.

The outcomes of the CIP project will also serve as important aspects of crisis management policy to be developed. Moreover, new infrastructures that can withstand all manner of disasters serve as a key cornerstone of crisis management. Starting in June 2004, the ministry of the Interior will place the protection of critical infrastructures in the hands of a new directorate within the line organisation, which will take over the management and co-ordination role currently fulfilled by the ministry of the Interior project organisation.

Published by
Ministry of the Interior and Kingdom Relations
National Coordination Centre
Postbus 20011
2500 EA Den Haag
The Netherlands

T +31 70 426 60 38
E info@minbzk.nl
I www.minbzk.nl

March 2004
VM53/24618